**UNITED STATES DISTRICT COURT**

**SOUTHERN DISTRICT OF NEW YORK**

ELAINE MALINOWSKI, individually, and on behalf of all others similarly situated,

Plaintiff,

vs.

MONUMENT, INC.,

Defendant.

**Case No.** 23-cv-3411

**CLASS ACTION COMPLAINT**

**[JURY TRIAL DEMANDED]**

Representative Plaintiff alleges as follows:

## INTRODUCTION

1. Representative Plaintiff Elaine Malinowski ("Representative Plaintiff") brings this class action against Defendant Monument, Inc. ("Defendant" or "Monument") to address Defendant's transmission of Representative Plaintiff's protected health information and personally identifiable information to unauthorized third parties such as Meta Platforms, Inc. d/b/a Meta ("Facebook") and/or Google LLC d/b/a Google ("Google") via a tracking pixel ("Tracking Pixel" or "Pixel") installed on Defendant's website.

2. Representative Plaintiff's and Class Members' information unlawfully intercepted and transmitted by Defendant includes, without limitation, full names, dates of birth, email addresses, telephone numbers, addresses, Monument identification numbers, insurance member identification numbers, IP addresses, unique digital identification numbers, Uniform Resource Locators, photographs, selected services or plans, assessments or survey responses, appointment-

related information and associated health information (these types of information, *inter alia*, being thereafter referred to collectively as "protected health information" or "PHI"[1] and "personally identifiable information" or "PII").[2]

3. According to its report submitted to the United States Department of Health and Human Services, Defendant admits that the PHI/PII of at least 108,584[3] individuals was improperly and unlawfully disclosed to third parties such as Facebook and Google without those individuals' knowledge or consent.

4. Defendant is an online web platform that hosts access to healthcare providers and therapists specializing in treating alcohol dependency. Defendant offers a subscription service to its website that includes regular therapy and online, anonymous forums for clients to get support from other clients.[4] In doing so, Defendant collected sensitive PHI/PII.

5. Representative Plaintiff further seeks to hold Defendant responsible for not ensuring that PHI/PII was maintained in a manner consistent with industry, the Health Insurance Portability and Accountability Act of 1996 ("HIPPA") Privacy Rule (45 CFR, Part 160 and Parts A and E of Part 164), the HIPPA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) and other relevant standards.

---

1 Personal health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

2 Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

3 "*U.S. Department of Health and Human Services, Breach Portal,"* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf/ (last accessed April 18, 2023).

4 "*Monument,*" https://joinmonument.com/ (last accessed April 17, 2023).

6. Defendant disclosed Representative Plaintiff's and Class Member's PHI/PII via the Tracking Pixel to third parties. Defendant's disclosure of Representative Plaintiff's and Class Members' Private Information constitute as gross violation of common law and statutory data privacy laws.

7. Defendant did not acknowledge that the Tracking Pixel and its widespread and blatant disclosures of Representative Plaintiff's and Class Members' PHI/PII until March 31, 2023.

8. On March 31, 2023 Defendant sent a letter to Representative Plaintiff (hereinafter referred to as the "Notice of Data Security Incident"), which states the following:

> We value and respect the privacy of our members' information, which is why Monument, Inc. ("Monument") is writing to inform you of a recent incident that may have involved your personal information – and let you know about the steps we have taken and that you can take to protect such information.
>
> Monument owns and operates both the Monument and Tempest website, to which you have visited or on which you created an account. These websites, like many others, used technologies known commonly as "pixels" or other similar technologies known as "tracking technologies." Common examples of tracking technologies are those made available by Meta (Facebook), Google, Bing, Pinterest, as well as other third parties. In late 2022, the federal government issued guidance on the uses of those online tracking technologies, and Monument promptly undertook an internal review to determine whether and how we should change our practices to better protect member privacy.
>
> As a result of our internal review, Monument has stopped using tracking technologies offered by third parties like those services named above. On or about February 6, 2023, Monument's internal review concluded that some information may have been shared with those third parties without the appropriate authorization, consent, or agreements required by law. The internal review concluded that this activity commenced in January 2020, with respect to Monument members, and November of 2017, with respect to Tempest members. The information shared may have included name, date of birth, email address, telephone number, address, Monument ID, insurance member ID, IP address, unique digital ID, Uniform Resource Locator (URL), photograph, selected services or plan, assessment or survey responses, appointment-related information, and associated health

> information. Monument stopped using most tracking technologies in late 2022 and fully disconnected the Monument websites from these third-party tracking technologies by February 23, 2023.
>
> Not every member provided the same amount of information to the Monument website, so whether your specific information was shared with a third party depends on what actions you took on the Monument website, the configuration of the tracking technologies when you visited the Monument websites, and how the web browser on your computer or mobile device was configured, among other factors. Please note that the information involved did not include your Social Security number or credit or debit card information.
>
> Out of an abundance of caution, and because we want to be transparent with our members, Monument is notifying all members, even those members that may not have created an account or become a patient of Monument or Tempest's affiliated medical groups, Live Life Now Health Group and Purdy medical Corp. Monument is committed to only sharing information in a manner that complies with HIPAA and all other applicable law. Monument has removed tracking technologies from the Monument websites and will only engage with third-party vendors able to meet the requirements of HIPAA and other applicable privacy laws.

9. Defendant has admitted that its website contained a Tracking Pixel that secretly enabled the unauthorized transmission and disclosure of Representative Plaintiff's and Class Members' PHI/PII to third parties such as Facebook or Google.

10. Defendant also acknowledged that the Notice of Data Security Incident pertains to both patients and those who merely accessed the website without creating an account.

11. Third parties, such as Facebook or Google, in turn, use Representative Plaintiff's and Class Member's PHI/PII to target advertisements to Representative Plaintiff and Class Members based on the PHI/PII disclosed by Representative Plaintiff and Class Members to Defendant.

12. Accordingly, the purpose of this lawsuit is to protect Representative Plaintiff's and Class Members' rights to protect their PHI/PII and seek remedies for the harm caused by

Defendant's intentional, reckless or negligent disclosure to third parties such as Facebook and/or Google.

## JURISDICTION AND VENUE

13. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member is a citizen of a state different from Defendant.

14. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

15. Defendant is headquartered and routinely conducts business in the State where this District is located, has sufficient minimum contacts in this State and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

16. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Representative Plaintiff's claims took place within this District, and Defendant does business in this Judicial District.

## PLAINTIFF

17. Representative Plaintiff is an adult individual and, at all relevant times herein, a resident and citizen of the State of Florida. Representative Plaintiff is a victim of the Data Security Incident (as further defined below).

18. Defendant received highly sensitive personal and medical information from Representative Plaintiff in connection with the medical services Representative Plaintiff received or requested. As a result, Representative Plaintiff's information was among the data transmitted to unauthorized third parties by Defendant.

19. Representative Plaintiff received—and was a "consumer"—for purposes of obtaining services from Defendant within this State.

20. At all times herein relevant, Representative Plaintiff is and was a member of each of the Classes.

21. As required in order to obtain services from Defendant, Representative Plaintiff provided Defendant with highly sensitive personal, financial, health and insurance information.

22. Representative Plaintiff's PHI/PII was exposed vis-a-vis the Tracking Pixel on Defendant's website and subject to Defendant's willful transmission because Defendant stored and/or shared Representative Plaintiff's PHI/PII. Representative Plaintiff's PHI/PII was within the possession and control of Defendant.

23. Representative Plaintiff received a letter from Defendant, dated March 31, 2023, stating Representative Plaintiff PHI/PII had been exposed vis-a-vis Defendant's Tracking Pixel (the "Data Security Incident").

24. As a result, Representative Plaintiff spent time dealing with the consequences of the Data Security Incident, which included and continues to include time spent verifying the legitimacy and impact of the Data Security Incident, exploring credit monitoring and identity theft insurance options, self-monitoring Representative Plaintiff's accounts and seeking legal counsel regarding Representative Plaintiff's options for remedying and/or mitigating the effects of the Data Security Incident. This time has been lost forever and cannot be recaptured.

25. Representative Plaintiff suffered actual injury in the form of damages to and diminution in the value of Representative Plaintiff's PHI/PII—a form of intangible property that Representative Plaintiff entrusted to Defendant, which was compromised in and as a result of Defendant's transmission of the data vis-a-vis its Tracking Pixel.

26. Representative Plaintiff suffered lost time, annoyance, interference and inconvenience as a result of the Data Security Incident and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Representative Plaintiff's PHI/PII.

27. Representative Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Representative Plaintiff's PHI/PII in combination with Representative Plaintiff's name being placed in the hands of unauthorized third parties.

28. Representative Plaintiff has a continuing interest in ensuring that Representative Plaintiff's PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future transmissions.

## DEFENDANT

29. Defendant is a Delaware corporation with a principal place of business located at 350 Seventh Avenue, Suite 600, New York, New York 10001. Defendant hosts a telehealth platform to provide treatment for alcohol dependency. Defendant advertises itself as "the gold standard in alcohol treatment," and regularly mentions its high degree of "secure and confidential" treatment on its website.[5]

[5] "*Monument,*" https://joinmonument.com/ (last accessed April 17, 2023).

30. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiff. Representative Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of such Representative Plaintiff's responsible parties when its identities become known.

## CLASS ACTION ALLEGATIONS

31. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on Representative Plaintiff's own behalf and on behalf of the following classes/subclass(es) (collectively, the "Classes"):

> **Nationwide Class:**
> "All individuals within the United States of America whose PHI/PII was transmitted to unauthorized third parties by Defendant vis-a-vis its use of a tracking pixel disclosed in March of 2023."
>
> **Florida Subclass:**
> "All individuals within the State of Florida whose PHI/PII was transmitted to unauthorized third parties by Defendant vis-a-vis its use of a tracking pixel disclosed in March of 2023."

32. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including, but not limited to, its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

33. Also, in the alternative, Representative Plaintiff requests additional Subclasses as necessary based on the types of PHI/PII that were compromised.

34. Representative Plaintiff reserve the right to amend the above definition(s) or to propose subclasses in subsequent pleadings and motions for class certification.

35. This action has been brought and may properly be maintained as a class action under Federal Rules of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the Proposed Classes is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiff is informed and believes and, on that basis, alleges that the total number of Class Members is in the thousands of individuals. Membership in the classes will be determined by analysis of Defendant's records.

b. Commonality: Representative Plaintiff and the Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Defendant had a legal duty to Representative Plaintiff and the Classes to exercise due care in collecting, storing, using and/or safeguarding their PHI/PII;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Security Incident to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;

6) Whether Defendant adequately, promptly and accurately informed Representative Plaintiff and Class Members that their PHI/PII had been compromised;

7) How and when Defendant actually learned of the Data Security Incident;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PHI/PII of Representative Plaintiff and Class Members;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Security Incident to occur;

10) Whether Representative Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;

11) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Representative Plaintiff's claims are typical of the claims of the Plaintiff Classes. Representative Plaintiff and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiff in this class action is an adequate representative of each of the Plaintiff Classes in that the Representative Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in its entirety. Representative Plaintiff anticipates no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Classes the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

36. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes in their entireties. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiff's challenge of these policies and practices hinges on Defendant's conduct with respect to the Classes in their entireties, not on facts or law applicable only to Representative Plaintiff.

37. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure Class Members' PHI/PII, and Defendant may continue to act unlawfully as set forth in this Complaint.

38. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

## COMMON FACTUAL ALLEGATIONS

### Background

39. When an individual visits Defendant's website and submits PHI/PII to Defendant, its Tracking Pixel transmits that PHI/PII to third parties, such as Facebook and Google. A pixel is a piece of code that "tracks the people and [the] type of actions they take."[6] Pixels are routinely

[6] "*Meta, Retargeting,"* https://www.facebook.com/business/goals/retargeting/ (last accessed April 21, 2023).

used to target specific customers by utilizing the data gathered through Defendant's pixel to build profiles for the purposes of "retargeting"[7] and future marketing.

40. As an example, with respect to Facebook, the omnipresent Facebook Pixel on Defendant's website causes that individual's unique and persistent Facebook ID ("FID") to be transmitted alongside other PHI/PII that is sent to Facebook.

41. Upon information and belief, Defendant utilized the Pixel data to improve and save costs on its marketing campaigns, improve its data analytics, attract new patients, and market new services and/or treatments to its existing patients. In other words, Defendant implemented the Tracking Pixel to bolster its profits.

42. Pixels are routinely used to target advertising to specific customers by utilizing the data gathered through the pixel to build profiles for the purposed of retargeting and future marketing.

43. In this context, the Tracking Pixel is designed to report to third parties data gathered about the web page currently visited and any information to/from the User to the web page.

44. Operating as designed, Defendant's Tracking Pixel allowed Representative Plaintiff's and Class Members' PHI/PII submitted to Defendant to be unlawfully disclosed to third parties.

45. Indeed, when Representative Plaintiff or a Class Member accessed Defendant's website hosting the Pixel, the Pixel software directed Plaintiff's or the Class Member's browser to send a message to the third party's servers. The information sent to a third party by Defendant included the PHI/PII that Representative Plaintiff and/or the Class Member submitted to

[7] "Retargeting" or "remarketing" is a form of advertising that displays ads or sends emails to previous visitors of a particular website who did not "convert" the visit into a sale or otherwise meet the website owner's marketing goal.

Defendant's website, including, for example, the type and date of a medical appointment and physician. Such information would allow a third party (e.g., Facebook or Google) to know that a specific patient was seeking confidential medical care and the type of medical care being sought. Given Defendant's normal operations as an alcohol addiction recovery company, this disclosure would allow a third party to reasonably infer that a specific patient was being treated for alcoholism/alcohol dependency.

46. The third party, in turn, sells this PHI/PII to third-party marketers who online target[8] Representative Plaintiff and Class Members based on communications obtained via the Tracking Pixel.

47. Representative Plaintiff submitted medical information to Defendant's website and used the website to search for therapists, schedule appointments, receive and discuss medical diagnoses and treatment, exchange insurance information and discuss sensitive medical topics with other, anonymous patients.

48. Vis-a-vis the Tracking Pixel, Defendant transmitted this PHI/PII to third parties, such as Facebook and Google.

49. Defendant regularly encouraged Representative Plaintiff and Class Members to use its digital tools to receive healthcare services. In doing so, Defendant also directed Representative Plaintiff and Class Members to its Privacy Policies, which preclude the transmission or disclosure of HIPAA protected PHI/PII to unauthorized third parties, such as Facebook or Google.

[8] "Online Targeting" is "a process that refers to creating advertisement elements that specifically reach out to prospects and customers interested in offerings. A target audience has certain traits, demographics, and other characteristics, based on products or services the advertiser is promoting." See https://digitalmarketinggroup.com/a-guide-to-online-targeting-which-works-for-your-business/ (last visited: April 21, 2023).

50. Representative Plaintiff and Class Members provided PHI/PII to Defendant in order to receive medical services and with the reasonable expectation that Defendant would protect their PHI/PII.

51. At all times that Representative Plaintiff and Class Members visited and utilized Defendant's website, they had a reasonable expectation of privacy of the PHI/PII collected through Defendant's website, including that it would remain secure and protected and only utilized for medical purposes. Representative Plaintiff's and Class Members' expectations were entirely reasonable because (1) they are patients, (2) Defendant is a business associate of a healthcare provider and (3) is required by common and statutory law to protect its patients' PHI/PII. Moreover, Representative Plaintiff and Class Members relied on Defendant's Privacy Policy, which does not permit the identifiable transmission of Representative Plaintiff's and Class Member's PHI/PII to unauthorized third parties.

52. Defendant further made express and implied promises to protect Representative Plaintiff's and Class Member's PHI/PII and maintain the privacy and confidentiality of communications that patients exchange with Defendant or its affiliates.

53. Defendant owed common law, contractual, statutory and regulatory duties to keep Representative Plaintiff's and Class Members' Private Information safe, secure and confidential. Furthermore, by obtaining, collecting, using and deriving a benefit from Representative Plaintiff's and Class Members' PHI/PII, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized disclosure.

54. However, as set forth more fully below, Defendant failed in its obligations and promises by utilizing the Tracking Pixel on its website knowing that such technology would transmit and disclose Plaintiff's and Class Members' PHI/PII to unauthorized third parties.

55. Representative Plaintiff's and Class Members' exposed PHI/PII can—and likely will—be further disseminated to additional third parties utilizing the data for retargeting or to insurance companies utilizing the information to set insurance rates.

56. While Defendant willfully and intentionally incorporated the Tracking Pixel into its website, Defendant did not disclose to Representative Plaintiff or Class Members that it shared their sensitive and confidential communications vis-a-vis the Tracking Pixel to Facebook or Google until on or around March 31, 2023. As a result, Representative Plaintiff and Class Members were unaware that their PHI/PII was being surreptitiously transmitted and/or disclosed to Facebook and Google as they communicated with their healthcare provider via the website.

57. Defendant breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web based technology to ensure Defendant's website was safe and secure, (ii) failing to remove or disengage technology that was known and designed to share web-users' information, (iii) failing to obtain the consent of Representative Plaintiff and Class Members to disclose their PHI/PII to Facebook, Google or others, (iv) failing to take steps to block the transmission of Representative Plaintiff's and Class Members' Private Information through steps to block the transmission of Representative Plaintiff's and Class Members' PHI/PII vis-a-vis Tracking Pixels, (v) failing to warn Representative Plaintiff and Class Members and (vi) otherwise failing to design and monitor its website to maintain the confidentiality and integrity of patient PHI/PII.

58. Representative Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy, (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Tracking Pixel, (iii) loss of benefit of the bargain, (iv) diminution of value of the PHI/PII, (v) statutory damages, and

(vi) the continued and ongoing risk of exposure of their PHI/PII. Representative Plaintiff seeks to remedy these harms through this action.

**Defendant Improperly Disclosed PHI/PII Vis-a-Vis the Tracking Pixel**

59. Defendant utilizes its website to connect Representative Plaintiff and Class Members to Defendant's digital healthcare platform with the goal of increasing profitability.

60. To accomplish this, Defendant utilized the Tracking Pixel to advertise its services to Representative Plaintiff and Class Members. The Pixel is a piece of code that Defendant commonly used to secretly track patients by recording their activity and experiences on Defendant's website and electronic platforms.

61. While seeking and using Defendant's services as a medical provider, and utilizing the website, Representative Plaintiff's and Class Members' PHI/PII was intercepted in real time and then disseminated to Facebook, Google and, potentially, to other third parties, vis-a-vis the Pixel that Defendant secretly installed on its website.

62. Representative Plaintiff and Class Members did not intend or have any reason to suspect the PHI/PII would be shared with Facebook, Google, or other third parties, or that Defendant was tracking their every communication and disclosing same to third parties when they entered their PHI/PII on Defendant's website.

63. Defendant did not disclose to or warn Representative Plaintiff or Class Members that Defendant used Representative Plaintiff's and Class Members' confidential electronic medical communications and PHI/PII for marketing purposes.

64. Defendant tracked Representative Plaintiff's and Class Members' Private Information vis-a-vis the Tracking Pixel.

65. Representative Plaintiff and Class Members never consented to, agreed, authorized or otherwise permitted Defendant to disclose their PHI/PII.

66. Upon information and belief, Defendant intercepted and disclosed the following private information to third parties:

a. Representative Plaintiff's and Class Members' status as medical patients;

b. Representative Plaintiff's and Class Members' communications with Defendant through its website; and

c. Representative Plaintiff's and Class Member's therapy appointments, specific medical providers, specific medical conditions and treatments.

67. Defendant deprived Representative Plaintiff and Class Members of their privacy rights when it (i) implemented technology (i.e., the Tracking Pixel) that surreptitiously tracked, recorded, and disclosed Representative Plaintiff's and other online patients' confidential communications and PHI/PII, (ii) disclosed patients' protected information to Facebook, Google, and/or other unauthorized third-parties and (iii) undertook this pattern of conduct without notifying Representative Plaintiff or Class Members and without obtaining their express written consent.

**Defendant's Pixel, Source Code and Interception of HTTP Requests**

68. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as computer, tablet, or smart phone) accessed web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

69. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via their web browsers.

70. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies. These terms are defined as follows:

a. **HTTP Request:** an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.

b. **Cookies:** a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.

c. **HTTP Response:** an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

71. A patient's "HTTP Request," essentially, asks Defendant's website to retrieve certain information, and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's webpage(s)).

72. Every webpage is comprised of Markup and "Source Code." Source Code is a set of instructions invisible to the website's visitor that commands the visitor's browser to take certain actions when the webpage first loads or when a specified event triggers the code.

73. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendant's Pixel is source code that does just that. The Pixel acts much like a traditional wiretap. When patients visit Defendant's website via an HTTP Request to

Monument's server, Defendant's server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant's Pixel. Thus, Defendant is in essence handing patients a tapped phone, and once the Webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third-parties, including Facebook and Google.

74. Third parties, like Facebook or Google, place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third-party can uniquely identify the patient associated with the PHI/PII intercepted.

75. Thus, without any knowledge, authorization or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

76. In this case, Defendant employed just such a device to intercept, duplicate and re-direct Representative Plaintiff's and Class Members' Private Information to third parties like Facebook and Google.

**Defendant's Privacy Policy and Promises**

77. Defendant's Privacy Policy allows for the disclosure of aggregated information about its users (and information that does not identify any individual), and otherwise to comply with the law, to enforce its Terms of Use, or if disclosure is necessary to protect Defendant's rights, property or safety.[9]

[9] https://joinmonument.com/privacy-policy/ (last accessed April 21, 2023).

78. Defendant's Privacy Policy explicitly states that its disclosures are authorized only in aggregate and when the information does not identify any individual.

79. Representative Plaintiff and Class Members never provided Defendant with permission to share their identifying PHI/PII for marketing purposes.

80. Despite Defendant's acknowledgement that it would not share Representative Plaintiff's and Class Members' identifying PHI/PII, Defendant, in fact, shared Representative Plaintiff's and Class Members' identifying PHI/PII vis-a-vis the Tracking Pixel.

81. Specifically, Defendant transmitted and/or disclosed Representative Plaintiff's and Class Member's identifying PHI/PII, such as IP addresses, insurance numbers, full names and addresses to third parties such as Facebook or Google without authorization.

82. In doing so, Defendant intended to improve and save costs on its marketing campaign, improve its data analytics, attract new patients and market new services and/or treatments to its existing patients.

83. In simple terms, Defendant violated its own Privacy Policy—i.e., the Privacy Policy that Representative Plaintiff and Class Members relied upon—in order to bolster its profits.

**Defendant Violated HIPAA Standards**

84. Under Federal Law, a healthcare provider or covered business associate may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization. HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

85. Guidance from the United States Department of Health and Human Services instructs healthcare providers and covered business associates that patient status alone is protected by HIPAA.

86. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[10]

87. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.[11]

88. In addition, the Office for Civil Rights ("OCR") at the U.S. Department of Health and Human Services ("HHS") has issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and

[10] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last accessed April 21, 2023).

[11] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last accessed April 21, 2023).

Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[12]

89. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

90. Thus, HHS has expressly stated that Defendant has violated HIPAA Rules by implementing the Tracking Pixel.

**Representative Plaintiff's and Class Member's Expectation of Privacy**

91. Representative Plaintiff and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

92. Indeed, at all times when Representative Plaintiff and Class Members provided their PHI/PII to Defendant, they had a reasonable expectation that the information would remain private and that Defendant would not share the PHI/PII with third parties for a commercial purpose, unrelated to patient care.

**Defendant was Enriched from the Use of the Pixel and Unauthorized Disclosures**

93. The sole purpose of the use of the Tracking Pixel on Defendant's Website was better marketing and profits.

94. In exchange for disclosing the Private Information of its patients, Defendant is compensated by third parties, like Facebook and Google, in the form of enhanced advertising services and more cost-efficient marketing on Facebook.

[12] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html/ (last accessed April 21, 2023).

95. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

96. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients, including Representative Plaintiff and Class Members.

97. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby financially benefitting Defendant.

**Value of the Relevant Sensitive Information**

98. Electronic health records, such as those collected and transmitted vis-a-vis Defendant's Pixel, contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, RX's, treatment plans) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on a number of underground internet websites. Unsurprisingly, the healthcare industry is at high risk for and acutely affected by cyberattacks.

99. The high value of PHI/PII to criminals is further evidenced by the prices they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[13] Experian reports that a stolen credit or debit

[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 28, 2021).

card number can sell for $5 to $110 on the dark web.[14] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[15]

100. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiff and Class Members. For example, it is believed that certain PHI/PII compromised in the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

101. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

102. Identity thieves can use PHI/PII, such as that of Representative Plaintiff and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with

[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed November 5, 2021).

[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed January 21, 2022).

another's picture, using the victim's information to obtain government benefits or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

103. The ramifications of Defendant's failure to keep secure Representative Plaintiff's and Class Members' PHI/PII are long lasting and severe. Once PHI/PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years.

104. There may be a time lag between when harm occurs versus when it is discovered, and also between when PHI/PII is exfiltrated and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

105. The harm to Representative Plaintiff and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[17]

106. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy

[16] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed January 21, 2022).
[17] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed January 21, 2022).

Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[18]

107. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[19] Almost half of medical identity theft victims lose its healthcare coverage as a result of the incident, while nearly one-third saw its insurance premiums rise, and forty percent were never able to resolve its identity theft at all.[20]

108. Defendant disregarded the rights of Representative Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusion, (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiff's and Class Members' PHI/PII, (iii) failing to take standard and reasonably available steps to prevent the transmission of PHI/PII, (iv) concealing the existence and extent of the Pixel's transmission for an unreasonable duration of time and (v) failing to provide Representative Plaintiff and Class Members prompt and accurate notice of the transmission of their PHI/PII.

---

[18] *Id*.

[19] See Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed January 21, 2022).

[20] Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed January 21, 2022).

**COUNT 1**
**INVASION OF PRIVACY**
**(On behalf of the Nationwide Class and the Florida Subclass)**

109. Each and every allegation of the preceding paragraphs is incorporated in this claim with the same force and effect as though fully set forth herein.

110. Representative Plaintiff and Class Members had a legitimate expectation of privacy to their PHI/PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

111. Defendant owed a duty to Representative Plaintiff and Class Members to keep their PHI/PII confidential.

112. Defendant failed to protect and released to unknown and unauthorized third parties Representative Plaintiff's and Class Members' PHI/PII.

113. Defendant allowed unauthorized and unknown third parties access to and examination of Representative Plaintiff's and Class Members' PHI/PII, by way of Defendant's willful and intentional disclosure of their PHI/PII to third parties.

114. The unauthorized release to, custody of and examination by unauthorized third parties of Representative Plaintiff's and Class Members' PHI/PII is highly offensive to a reasonable person.

115. The unauthorized intrusion was into a place or thing which was private and is entitled to be private. Representative Plaintiff and Class Members disclosed their PHI/PII and to Defendant as part of obtaining healthcare from Defendant, but privately with an intention that the PHI/PII would be kept confidential and would be protected from unauthorized disclosure. Representative Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without its authorization.

116. Defendant's conduct constitutes an intentional physical or sensory intrusion on Representative Plaintiff's and Class Members' privacy because Defendant facilitated Facebook's simultaneous eavesdropping and wiretapping of confidential communications.

117. Defendant failed to protect Representative Plaintiff's and Class Members' Private Information and acted knowingly when it incorporated the Tracking Pixel into its website because it knew the functionality and purpose of the Tracking Pixel.

118. Because Defendant intentionally and willfully incorporated the Tracking Pixel into its website and encouraged patients to use that website for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Representative Plaintiff and Class Members. As a proximate result of Defendant's acts and omissions, Representative Plaintiff's and Class Members' PHI/PII was disclosed to a third party without authorization, causing Representative Plaintiff and the Class to suffer damages.

119. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Representative Plaintiff and Class Members in that the PHI/PII maintained by Defendant can be viewed, distributed and used by unauthorized persons for years to come. Representative Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Representative Plaintiff and/or Class Members.

**COUNT 2**
**BREACH OF CONFIDENCE**
**(On behalf of the Nationwide Class and the Florida Subclass)**

120. Each and every allegation of the preceding paragraphs is incorporated in this claim with the same force and effect as though fully set forth therein.

121. At all times during Representative Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential nature of the PHI/PII that Representative Plaintiff and Class Members provided to it.

122. As alleged herein and above, Defendant's relationship with Representative Plaintiff and the Class Members was governed by promises and expectations that Representative Plaintiff and Class Members' PHI/PII would be collected, stored and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties.

123. Representative Plaintiff and Class Members provided their respective PHI/PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PHI/PII to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties.

124. Representative Plaintiff and Class Members also provided their PHI/PII to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect their PHI/PII from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use and/or viewing such as following basic principles of protecting its networks and data systems.

125. Defendant voluntarily received, in confidence, Representative Plaintiff's and Class Members' PHI/PII with the understanding that the PHI/PII would not be accessed by, acquired by,

appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by the public or any unauthorized third parties.

126. Contrary to its duties as a covered entity under HIPAA and its express promises of confidentiality, Defendant deployed the Tracking Pixel to disclose and transmit Representative Plaintiff's PHI/PII and the contents of their communications exchanged with Defendant to third parties.

127. The third-party recipients included, but were not limited to, Facebook and Google.

128. Defendant's disclosures of Representative Plaintiff's and Class Members' PHI/PII were made without their knowledge, consent or authorization, and were unprivileged.

129. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

130. As a direct and proximate cause of Defendant's actions and/or omissions, Representative Plaintiff and Class Members have suffered damages, as alleged herein.

131. The injury and harm Representative Plaintiff and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Representative Plaintiff's and Class Members' PHI/PII.

132. As a direct and proximate result of Defendant's breaches of confidence, Representative Plaintiff and Class Members have suffered and will suffer injury including, but not limited, to (a) actual identity theft, (b) the compromise, publication and/or theft of their PHI/PII, (c) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their PHI/PII, (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of Defendant's transmission of their PHI/PII, including, but not limited to, efforts

spent researching how to prevent, detect, contest and recover from identity theft, (e) the continued risk to their PHI/PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Class Members' PHI/PII in its continued possession, (f) future costs in terms of time, effort and money that will be expended as result of Defendant's transmission of PHI/PII for the remainder of Representative Plaintiff's and Class Members' lives, (g) the diminished value of Representative Plaintiff's and Class Members' PHI/PII and (h) the diminished value of Defendant's services for which Representative Plaintiff and Class Members paid and received.

**COUNT 3**
**BREACH OF IMPLIED CONTRACT**
**(On behalf of the Nationwide Class and the Florida Subclass)**

133. Each and every allegation of the preceding paragraphs is incorporated in this claim with the same force and effect as though fully set forth therein.

134. Through its course of conduct, Defendant, Representative Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Representative Plaintiff's and Class Members' PHI/PII.

135. Defendant required Representative Plaintiff and Class Members to provide and entrust their PHI/PII to it as a condition of obtaining Defendant's services.

136. Defendant solicited and invited Representative Plaintiff and Class Members to provide their PHI/PII to it as part of Defendant's regular business practices. Representative Plaintiff and Class Members accepted Defendant's offers and provided their PHI/PII to Defendant.

137. As a condition of being direct clients of Defendant, Representative Plaintiff and Class Members provided and entrusted their PHI/PII to Defendant. In so doing, Representative Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant

agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Representative Plaintiff and Class Members if their data had been breached and compromised or stolen.

138. A meeting of the minds occurred when Representative Plaintiff and Class Members agreed to, and did, provide their PHI/PII to Defendant, in exchange for, amongst other things, the protection of their PHI/PII.

139. Representative Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

140. Defendant breached the implied contracts it made with Representative Plaintiff and Class Members by failing to safeguard and protect their PHI/PII and by failing to provide timely and accurate notice to them that their PHI/PII was compromised as a result of the Data Security Incident.

141. As a direct and proximate result of Defendant's above-described breach of implied contract, Representative Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (c) loss of the confidentiality of the stolen confidential data, (d) the illegal sale of the compromised data on the dark web, (e) lost work time and (f) other economic and non-economic harm.

**COUNT 4**
**UNJUST ENRICHMENT**
**(On behalf of the Nationwide Class and the Florida Subclass)**

142. Each and every allegation of the preceding paragraphs is incorporated in this claim with the same force and effect as though fully set forth herein.

143. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Representative Plaintiff and Class Members.

144. Representative Plaintiff and Class Members conferred a benefit upon Defendant in the form of PHI/PII that Defendant collected from Representative Plaintiff and Class members and then disclosed to thirds parties without authorization and prior compensation. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible and other benefits, including substantial monetary compensation.

145. Defendant unjustly retained those benefits at Representative Plaintiff's and Class Members' expense because Defendant's conduct damaged Representative Plaintiff and Class Members, all without providing commensurate compensation to Representative Plaintiff and Class Members.

146. The benefits that Defendant derived from Representative Plaintiff and Class Members were not offered by Representative Plaintiff and Class Members gratuitously and rightly belong to Representative Plaintiff and Class Members. It would be inequitable under unjust enrichment principles in Florida (where Representative Plaintiff lives) and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts and trade practices alleged in this Complaint.

147. Defendant, prior to and at the time Representative Plaintiff and Class Members entrusted their PHI/PII to Defendant for the purpose of obtaining health services, caused

Representative Plaintiff and Class Members to reasonably believe that Defendant would keep such PHI/PII secure.

148. Defendant was aware or should have been aware that reasonable patients and consumers would have wanted their PHI/PII kept secure and would not have contracted with Defendant, directly or indirectly, had they known that Defendant intended to market their PHI/PII to third parties.

149. Defendant was also aware that, if it was disclosed that Defendant intended to market the PHI/PII it acquired from patients and consumers to third parties, it would negatively affect Representative Plaintiff's and Class Members' decisions to seek its services.

150. Defendant failed to disclose facts pertaining to its intentions, defects and vulnerabilities therein before Representative Plaintiff and Class Members made their decisions to make purchases, engage in commerce therewith and seek services or information. Instead, by concealing and suppressing that information, Defendant denied Representative Plaintiff and Class Members the ability to make rational and informed purchasing and health care decisions and took undue advantage of Representative Plaintiff and Class Members.

151. Defendant was unjustly enriched at the expense of Representative Plaintiff and Class Members. Defendant received profits, benefits and compensation, in part, at the expense of Representative Plaintiff and Class Members. By contrast, Representative Plaintiff and Class Members did not receive the benefit of their bargain because they paid for products and/or health care services that did not satisfy the purposes for which they bought and/or sought them.

152. Since Defendant's profits, benefits and other compensation were obtained by improper means, Defendant is not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

153. Representative Plaintiff and Class Members seek an Order of this Court requiring Defendant to refund, disgorge and pay as restitution any profits, benefits and other compensation obtained by Defendant from its wrongful conduct and/or the establishment of a constructive trust from which Representative Plaintiff and Class Members may seek restitution.

**COUNT 5**
**ELECTRONIC COMMUNICATIONS PRIVACY ACT**
**VIOLATION OF 18 U.S.C. § 2511, *ET SEQ.***
**(On behalf of the Nationwide Class and the Florida Subclass)**

154. Each and every allegation of the preceding paragraphs is incorporated in this claim with the same force and effect as though fully set forth herein.

155. The Electronic Communications Privacy Act of 1986 ("ECPA") protects both sending and receipt of communications.

156. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed or intentionally used in violation of Chapter 119.

157. The transmissions of Representative Plaintiff's and Class Members' PHI/PII to Defendant website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

158. **Electronic Communications.** The transmission of PHI/PII between Representative Plaintiff and Class Members and Defendant's website with which they chose to exchange communications are "transfer[s] of signs, signals, writings. […] data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

159. **Content.** The ECPA defines content, when used with respect to electronic communications, to "[include] *any* information concerning the substance, purport or meaning of that communication." 18 U.S.C. § 2510(8).

160. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical , or other device" and "contents […] include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

161. **Electronic, Mechanical or Other Device.** The ECPA defines "electronic, mechanical, or other device" as "any device […] which can be used to intercept a[n] […] electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Representative Plaintiff's and Class Member's browsers;

b. Representative Plaintiff's and Class Members' computing devices;

c. The Pixel code deployed by Defendant to effectuate the sending the acquisition of patient communications.

162. By utilizing and embedding the Pixel on its website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept Representative Plaintiff's and Class Members' electronic communications, in violation of 18 U.S.C. § 2511(1)(a).

163. Specifically, the Defendant intercepted Representative Plaintiff's and Class Members' electronic communications vis-a-vis the Tracking Pixel, which tracked, stored and unlawfully disclosed Representative Plaintiff's and Class Members' PHI/PII to third parties such as Facebook and Google.

164. Defendant's intercepted communications include, but are not limited to, communications to/from Representative Plaintiff's and Class Members' regarding PHI/PII, treatment, medication and scheduling.

165. By intentionally disclosing or endeavoring to disclose Representative Plaintiff's and Class Members' electronic communications to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

166. By intentionally using or endeavoring to use the contents of Representative Plaintiff's and Class Members' electronic communications, while knowing or having reason to know that the information was obtained through the interceptions of an electronic communication in violation 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

167. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of Representative Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

168. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track the utilize Representative Plaintiff's and Class Members' PHI/PII for financial gain.

169. Defendant was not acting under color of law to intercept Representative Plaintiff's and/or Class Members' wire or electronic communication.

170. Representative Plaintiff's did not authorize Defendant to acquire the content of their communications for purposes of invading Representative Plaintiff's and/or Class Members' privacy vis-a-vis the Pixel tracking code.

171. Any purported consent that Defendant received from Representative Plaintiff's and/or Class Members was invalid.

172. By sending and by acquiring the content the Representative Plaintiff's and/or Class Members' communications relating to the browsing of Defendant's website, Defendant's purpose was tortious, criminal and designed to violate federal and state legal provisions, including those described herein, and constitute a knowing intrusion into a private place, conversation or matter that would be highly offensive to a reasonable person.

**COUNT 6**
**ELECTRONIC COMMUNICATIONS PRIVACY ACT**
**VIOLATION OF 18 U.S.C. § 2511(3)**
**(On behalf of the Nationwide Class and the Florida Subclass)**

173. Each and every allegation of the preceding paragraphs is incorporated in this claim with the same force and effect as though fully set forth herein.

174. The Electronic Communications Privacy Act of 1986 ("ECPA") provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

175. **Electronic Communication Service.** An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

176. Defendant's website is an electronic communication service. The website provides to users thereof the ability to send to receive electronic communications. In the absence of Defendant's website, internet user could not send or receive communications regarding Representative Plaintiff's and Class Members' PHI/PII.

177. **Intentional Divulgence.** Defendant intentionally designed the Tracking Pixel and was or should have been aware that, if misconfigured, it could divulge Representative Plaintiff's and Class Members' PHI/PII.

178. **While in Transmission.** Upon information and belief, Defendant's divulgence of the contents of Representative Plaintiff's and Class Members' communications was contemporaneous with their exchange with Defendant's website to which they directed their communications.

179. Defendant divulged the contents of Representative Plaintiff's and Class Members' electronic communications without authorization. Defendant divulged the contents of Representative Plaintiff's and Class Members' communications to Facebook without Representative Plaintiff's and Class Members' consent and/or authorization.

180. **Exceptions do not apply.** In addition to the exception for communication directly to an ECS or an agent of an ECS, 18 U.S.C. § 2511(3)(b) states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication as follows:

a. as otherwise authorized in section 2511(2)(a) or 2517 of this title;

b. with the lawful consent of the originator or any addressee or intended recipient of such communication;

c. to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

d. which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such a divulgence is made to a law enforcement agency."

181. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged to any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of a wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

182. Defendant's divulgence of the contents of Representative Plaintiff's and Class Members' communications on Defendant's website to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (i) a necessary incident to the rendition of Defendant's service or (ii) necessary to the protection of the rights or property of Defendant.

183. Defendant's divulgence of the contents of user communications on Defendant's browser through the Pixel code was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." 18 U.S.C. § 2702(b). As alleged above, (i) Representative Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications, and (ii) Defendant did not procure the "lawful consent" from the website with which Representative Plaintiff and Class Members were exchanging information.

184. Moreover, Defendant divulged the contents of Representative Plaintiff's and Class Members' communication through the Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

185. The contents of Representative Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

186. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages, preliminary and equitable or declaratory relief as may be appropriate, punitive damages in an amount to be determined by a jury, and reasonable attorneys' fees and other litigation costs reasonably incurred.

**COUNT 7**
**ELECTRONIC COMMUNICATIONS PRIVACY ACT**
**VIOLATION OF 18 U.S.C. § 2702, *ET SEQ.***
**(On behalf of the Nationwide Class and the Florida Subclass)**

187. Each and every allegation of the preceding paragraphs is incorporated in this claim with the same force and effect as though fully set forth herein.

188. The Electronic Communications Privacy Act of 1986 ("ECPA") further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

189. Defendant intentionally procures and embeds various PHI/PII through the Pixel code used on Defendant's website, which qualifies as an "electronic communication service."

190. **Electronic Storage.** ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

191. Defendant stores the content of Representative Plaintiff's and Class Members' communications on Defendant's website and files associated with it.

192. When Representative Plaintiff or Class Members make a website communication, the content of that communication is immediately placed into storage.

193. Defendant knowingly divulges the contents of Representative Plaintiff's and Class Members' communications from electronic storage.

194. **Exceptions Do Not Apply**. Section 2702(b) of the Stored Communications Act provides that an electronic communication service provider "may divulge the contents of a communication:"

a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient";

b. "as otherwise authorized in Section 2517, 25111(2)(a), or 2703 of this title";

c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service";

d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination";

e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service";

f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A";

g. "to a law enforcement agency, if the contents (i) were inadvertently obtained by the service provider, and (ii) appear to pertain to the commission of a crime";

h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or

i. "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfied Section 2523."

195. Defendant did not divulge the contents of Representative Plaintiff's and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Representative Plaintiff and/or Class Members.

196. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose or use that communication in the normal course of the employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

197. Defendant's divulgence of the contents of Representative Plaintiff's and Class Members' communications on Defendant's website to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither (i) a necessary incident to the rendition of Defendant's services, nor (ii) necessary to the protection of the rights or property of Defendant.

198. Defendant's divulgence of the contents of user communications on Defendant's website was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." 18 U.S.C. § 2511(3)(a). As alleged above, (i) Representative Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications, and (ii) Defendant did not procure the "lawful consent" from the website with which Representative Plaintiff and Class Members were exchanging information.

199. Moreover, Defendant divulge the contents of Representative Plaintiff's and Class Members' communications through the Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

200. The contents of Representative Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of the communications to a law enforcement agency.

201. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages, preliminary and other equitable or declaratory relief as may be appropriate, punitive damages in an amount to be determined by a jury, and reasonable attorneys' fees and other litigation costs reasonably incurred.

**COUNT 8**
**VIOLATION OF COMPUTER FRAUD AND ABUSE ACT**
**18 U.S.C. § 1030, *et seq.***
**(On behalf of the Nationwide Class and the Florida Subclass)**

202. Each and every allegation of the preceding paragraphs is incorporated in this claim with the same force and effect as though fully set forth herein.

203. Representative Plaintiff's and Class Members' mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are, therefore, protected computers" under 18 U.S.C. § 1030(e)(2)(B).

204. Defendant exceeded and continues to exceed authorized access to the Representative Plaintiff's and Class Members' protected computers and obtained information thereby, in violation of the Computer Fraud and Abuse Act of 1986 ("CFAA"); 18 U.S.C. § 1030(a)(2), (a)(2)(C).

205. Defendant's conduct caused "loss to 1 or persons during any 1-year period […] aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Representative Plaintiff's and Class Members' PHI/PII—including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text

box) URLs of web pages visited and/or electronic communications in real-time which were never intended for public consumption.

206. Defendant's conduct also constitutes a "threat to public safety" under 18 § U.S.C. 1030(c)(4)(A)(i)(IV) due to Representative Plaintiff's and Class Members' PHI/PII being made available to Defendant and other third parties without adequate legal privacy protections.

207. Accordingly, Representative Plaintiff and Class Members are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

**COUNT 9**
**FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT**
**Fla. Stat. §§ 501.201, *et seq.***
**(On behalf of the Florida Subclass)**

208. Each and every allegation of the preceding paragraphs is incorporated in this claim with the same force and effect as though fully set forth herein.

209. Representative Plaintiff and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

210. Defendant advertised, offered or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

211. Defendant engaged in unconscionable, unfair and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Representative Plaintiff and Florida Subclass Members' PII/PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks and adequately maintain and/or improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Representative Plaintiff and Florida Subclass

Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.,* and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Representative Plaintiff and Florida Subclass Members' PII/PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Representative Plaintiff and Florida Subclass Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.,* and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure Representative Plaintiff and Florida Subclass Members' PII/PHI; and

g. Omitting, suppressing and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Representative Plaintiff and Florida Subclass Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.,* and Florida's data security statute, F.S.A. § 501.171(2).

212. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII/PHI.

213. Had Defendant disclosed to Representative Plaintiff and Florida Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant held itself out as a large, sophisticated corporation with the resources to put adequate data security protocols in place–indeed, a "trusted adviser"–that could be trusted with valuable PII/PHI regarding thousands of consumers, including Representative Plaintiff and the Florida Subclass. Defendant accepted the responsibility while keeping the inadequate state of its security controls secret from the public. Accordingly, because Defendant held itself out as having the ability to maintain a secure environment for users' email accounts with a corresponding duty of trustworthiness and care, Representative Plaintiff and the

Florida Subclass Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

214. As a direct and proximate result of Defendant's unconscionable, unfair and deceptive acts and practices, Representative Plaintiff and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and nonmonetary damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft and loss of value of their PII/PHI.

215. Representative Plaintiff and Florida Subclass Members seek all monetary and nonmonetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21, declaratory and injunctive relief, reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1) and any other relief that is just and proper.

**COUNT 10**
**VOLUNTARY DISCLOSURE OF CUSTOMER COMMUNICATIONS OR RECORDS**
**Fla. Stat. §§ 934.22, *et seq.***
**(On behalf of the Florida Subclass)**

216. Each and every allegation of the preceding paragraphs is incorporated in this claim with the same force and effect as though fully set forth herein.

217. Representative Plaintiff and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

218. Florida Stat. § 934.22(1). further provides that "[a] provider of electronic communication service to the public may not knowingly divulge to: 1. Any person or entity the contents of a communication while in electronic storage by that service…."

219. Defendant intentionally procures and embeds various PHI/PII through the Pixel code used on Defendant's website, which qualifies as an "electronic communication service."

220. Defendant stores the content of Representative Plaintiff's and Florida Subclass Members' communications on Defendant's website and files associated with it.

221. When Representative Plaintiff and Florida Subclass Members make a website communication, the content of that communication is immediately placed into storage.

222. Defendant knowingly divulges the contents of Representative Plaintiff's and Florida Subclass Members' communications from electronic storage.

223. Defendant's divulgence of the contents of user communications on Defendant's website was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." Fla Stat. § 934.22(2)(c). As alleged above, (i) Representative Plaintiff and Florida Subclass Members did not authorize Defendant to divulge the contents of their communications, and (ii) Defendant did not procure the "lawful consent" from the website with which Representative Plaintiff and Florida Subclass Members were exchanging information.

224. Moreover, Defendant divulge the contents of Representative Plaintiff's and Florida Subclass Members' communications through the Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination." Fla Stat. § 934.22(2)(d).

225. The contents of Representative Plaintiff's and Florida Subclass Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of the communications to a law enforcement agency.

226. As a result of the above actions and pursuant to Fla Stat. § 934.27, the Court may assess statutory damages (i.e., no less than $1,000 per Florida Subclass Member), preliminary and other equitable or declaratory relief as may be appropriate, and reasonable attorneys' fees and other litigation costs reasonably incurred.

## RELIEF SOUGHT

**WHEREFORE,** Representative Plaintiff, individually, and on behalf of each member of the proposed National Class and the Florida Subclass, respectfully requests that the Court enter judgment in its/their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, statutory, nominal and consequential damages, as allowed by law in an amount to be determined;

3. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiff's and Class Members' PHI/PII, and from refusing to issue prompt, complete and accurate disclosures to Representative Plaintiff and Class Members;

4. For injunctive relief requested by Representative Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiff and Class Members, including, but not limited to, an Order:

   a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

   b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

   c. requiring Defendant to delete and purge the PHI/PII of Representative Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when

weighed against the privacy interests of Representative Plaintiff and Class Members;

d. prohibiting Defendant from maintaining Representative Plaintiff's and Class Members' PHI/PII on a cloud-based database;

e. requiring Defendant to conduct regular database scanning and securing checks;

f. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Representative Plaintiff and Class Members;

g. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

h. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

i. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

5. For punitive/exemplary damages in an amount appropriate and sufficient to punish Defendant and to deter others from engaging in similar misconduct in the future;

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs and litigation expenses, as allowed by law;

8. For all other Orders, findings and determinations identified and sought in this Complaint.

**JURY DEMAND**

Representative Plaintiff, individually, and on behalf of the Plaintiff Class(es) and/or Subclass(es), hereby demands a trial by jury for all issues triable by jury.

Dated: April 24, 2023

By: */s/ Joel H. Robinson*
Joel H. Robinson, Esq. (NY S.B. #2644607)
**ROBINSON YABLON COOPER & BONFANTE LLP**
232 Madison Ave.RM 909
New York, NY 10016
Telephone: (212) 725-8566

By: */s/ Scott Edward Cole*
Scott Edward Cole, Esq. (CA S.B. #160744) *
**COLE & VAN NOTE**
555 12th Street, Suite 1725
Oakland, California 94607
Telephone: (510) 891-9800
Email: sec@colevannote.com

By: */s/ Daniel Srourian*
Daniel Srourian, Esq. (CA S.B. #285678) *
**SROURIAN LAW FIRM, P.C.**
3435 Wilshire Blvd., Suite 1710
Los Angeles, California 90010
Telephone: (213) 474-3800
Email: daniel@slfla.com

Attorneys for Representative Plaintiff
and the Plaintiff Classes

**Pro hac vice forthcoming*